UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND

PETER MALDINI, KATHLEEN FRAKES HEVENER & TAMARA WALLACE, individually and on behalf of all others similarly situated, Plaintiffs, v. MARRIOTT INTERNATIONAL, INC., Defendant.	Case No. 1-18-cv-3841 COMPLAINT AND DEMAND FOR JURY TRIAL

Plaintiffs Peter Maldini, Kathleen Frakes Hevener, and Tamara Wallace, individually and on behalf of the other members of the below-defined nationwide class and statewide classes (collectively, the "Class"), hereby allege against Defendant Marriott International, Inc. ("Marriott"), parent of Starwood Hotels & Resorts Worldwide, LLC ("Starwood"), upon personal knowledge as to themselves and their own acts, and as to all other matters upon information and belief, based upon investigation of counsel, as follows:

I. INTRODUCTION

1. Marriott announced on November 30, 2018 that it was subject to one of the largest data breaches in our nation's history when unauthorized persons compromised the personal information of up to 500 million hotel guests from Marriott's Starwood guest reservation database as part of an ongoing, four-year long data breach.

2. Marriott failed to secure and safeguard its customers' personally identifiable information ("PII") such as the passport information, customers' names, mailing addresses, and other personal information, as well as credit and debit card numbers and other payment card data ("PCD") contained in Starwood's guest reservation database. Starwood and Marriott collected this information at the time customers registered on one of its hotel websites, checked-in to one of its hotels, used its loyalty program (the "Loyalty Program"), and/or used it at one of its dining or retail operations within its hotels.

3. During the four-year breach, Marriott failed to detect the hackers' presence, notice the massive amounts of data that was being stolen from its databases, or take any steps to investigate the numerous other red flags that should have warned the company about what was happening. As a result of Marriott's failure to protect the consumer information it was entrusted to safeguard, Plaintiffs and members of the Class have been exposed to fraud, identity theft, financial harm and, as detailed below, are subject to a heightened, imminent risk of such harm in the future. Marriott also failed to provide timely, accurate, and adequate notice to Plaintiffs and members of the Class that their PCD and PII had been stolen, as well as precisely what types of information were stolen.

II. JURISDICTION AND VENUE

4. This Court has jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d). The aggregated claims of the individual class members exceed $5,000,000.00, exclusive of interest and costs, and this is a class action in which more

than two-thirds of the proposed plaintiff class and Defendant Marriott are citizens of different states.

5. This Court has jurisdiction over Marriott as it (1) maintains its corporate headquarters in this District; (2) Marriott makes decisions regarding overall corporate governance and management with regards to the hotels that it owns or manages, including the security measures to protect its customers' Private Information, in this District; (3) it is authorized to conduct business throughout the United States, including Maryland; (4) it owns and operates many hotels throughout Maryland and the United States; (5) and it advertises in a variety of media throughout the United States, including Maryland. Via its business operations throughout the United States, Marriott intentionally avails itself of the markets within this state to render the exercise of jurisdiction by this Court just and proper.

6. Venue is proper in this District pursuant to 28 U.S.C. § 1391(a)(1) because a substantial part of the events and omissions giving rise to this action occurred in this District and because Marriott is headquartered in this District.

III. PARTIES

7. Plaintiff Peter Maldini is a citizen and resident of the State of Maryland. Mr. Maldini has been a member of Defendant's Loyalty Program for more than fifteen years. He provided his personal and confidential information to Defendant on the basis that they would keep his information secure, and employ reasonable and adequate security measures to ensure that hackers would not compromise his information, and

notify him promptly in the event of a breach. On December 6, 2018, Defendant provided him email notice that his information was compromised by the 2014-2018 Data Breach.

8. Plaintiff Kathleen Frakes Hevener has been a citizen and resident of the State of Florida since October 2017. Prior to October 2017, Ms. Hevener was a citizen and resident of the State of Maryland. Ms. Hevener has been a member of Defendant's Loyalty Program for more than ten years. She provided her personal and confidential information to Defendant on the basis that they would keep her information secure, and employ reasonable and adequate security measures to ensure that hackers would not compromise her information, and notify her promptly in the event of a breach. On December 6, 2018, Defendant provided her email notice that her information was compromised by the 2014-2018 Data Breach.

9. Plaintiff Tamara Wallace is a citizen and resident of the State of North Carolina. Ms. Wallace is a member of Defendant's Loyalty Program. She provided her personal and confidential information to Defendant on the basis that they would keep her information secure, and employ reasonable and adequate security measures to ensure that hackers would not compromise her information, and notify her promptly in the event of a breach. On December 6, 2018, Defendant provided her email notice that her information was compromised by the 2014-2018 Data Breach.

10. Marriott International, Inc. ("Marriott") is a Delaware corporation with its principal place of business in Bethesda, MD. Marriott primarily derives its revenues from hotel and restaurant operations. Starwood is now a wholly-owned subsidiary of Marriott.

IV. FACTUAL BACKGROUND

A. Marriott's Acquisition of Starwood

11. On November 16, 2015, Marriott and Starwood announced that the boards of directors for each company had approved a definitive merger agreement.[1] The $12.2 billion dollar deal, which eventually closed at $13.6 billion, was said to create the world's largest hotel company.[2]

12. The Marriott and Starwood Stockholders voted to approve the merger on April 8, 2016. By September 20, 2016, the Marriott and Starwood merger had completed all regulatory anti-trust reviews and the deal was officially closed on September 23, 2018.[3] Efforts in merging the two companies, including their guest databases, have continued throughout 2018.[4]

B. The 2014 to 2018 Data Breach

13. On Friday November 30, 2018, Marriott International Inc. disclosed that it had experienced one of the largest data breaches in United States history. The database for guest reservations within the Starwood properties was hacked by persons currently

---

[1] *Marriott International to Acquire Starwood Hotels & Resorts Worldwide, Creating the World's Largest Hotel Company*, Marriott International: News Center (November 16, 2015), http://news.marriott.com/2015/11/marriott-international-to-acquire-starwood-hotel

[2] Robin Sidel & Craig Karmin, *Starwood Reports Payment-Information Data Breach*, Wall Street Journal (Nov. 20, 2015 5:40 PM), https://www.wsj.com/articles/starwood-reports-payment-information-data-breach-1448033469.

[3] Starwood Acquisition & Historical Information, Marriott International, https://marriott.gcs-web.com/starwood (last visited Dec. 6, 2018.)

[4] Scott McCartney, *Inside the Marriott-Starwood Loyalty Program Turbulence*, Wall Street Journal (Nov. 28, 2018 9:40 AM), https://www.wsj.com/articles/inside-the-marriott-star wood-loyalty-program-turbulence-1543416010.

unknown and may have exposed the PII and PCD of up to 500 million guests from 2014 to 2018 (hereinafter the "2014-2018 Data Breach").[5]

14. The database contained information of approximately 500 million guests who made a reservation at a Starwood property.[6] "For approximately 327 million of these guests, the information includes some combination of name, mailing address, phone number, email address, passport number, Starwood Preferred Guest ('SPG') account information, date of birth, gender, arrival and departure information, reservation date, and communication preferences."[7]

15. The hackers were able to collect and copy data for many years before Marriott discovered the 2014-208 Data Breach. On September 8, 2018, an internal security tool alerted Marriott to an unauthorized attempt to access the Starwood guest reservation database.[8] Marriott then engaged security experts to investigate what had occurred.[9] The investigation discovered that hackers had compromised the Starwood reservation database by gaining unauthorized access since 2014.[10]

---

[5] Aisha Al-Muslin, Dustin Volz, & Kimberly Chin, *Marriott Says Starwood Data Breach Affects Up to 500 Million People*, Wall Street Journal (Nov. 30, 2018 8:02 PM), https://www.wsj.com/articles/marriotts-says-up-to-500-million-affected-by-starwood-breach-1543587121.

[6] *Marriott Announces Starwood Guest Reservation Database Security Incident*, Marriott International: News Center (November 30, 2018), http://news.marriott.com/2018/11/marriott -announces-starwood-guest-reservation-database-security-incident/.

[7] *Id.*

[8] *Id.*

[9] *Id.*

[10] *Id.*

16. The unauthorized party had copied and encrypted guests' PII and PCD stored in the database and saved the copied data into two massive data files.[11] The hackers also took steps to remove the copied data from the database.[12] Marriott is not able to verify whether the information was successfully removed from the network.[13] On November 19, 2018, Marriott decrypted the copied data files and determined that guests PII and PCD had been exposed.[14]

17. The 2014-2018 Data Breach was caused and enabled by Marriott's knowing violation of its obligations to abide by best practices and industry standards in protecting its customers' Private Information.

18. Hacking is often accomplished in a series of phases, including reconnaissance; scanning for vulnerabilities and enumeration of the network; gaining access; escalation of user, computer and network privileges; maintaining access; covering tracks; and placing backdoors. On information and belief, while hackers scoured Marriott's networks to find a way to access PCD, they had access to and

[11] *Id.*; Robert McMillan, *Marriott's Starwood Missed Chance to Detect Huge Data Breach Years Earlier, Cybersecurity Specialists Say*, Wall Street Journal (Dec. 2, 2018 5:11 PM), https://www.wsj.com/amp/articles/marriotts-starwood-missed-chance-to-detect-huge-data-breach-years-earlier-1543788659.

[12] *Marriott Announces Starwood Guest Reservation Database Security Incident*, Marriott International: News Center (November 30, 2018), http://news.marriott.com/2018/11/marriott-announces-starwood-guest-reservation-database-security-incident/.

[13] Robert McMillan, *Marriott's Starwood Missed Chance to Detect Huge Data Breach Years Earlier, Cybersecurity Specialists Say*, Wall Street Journal (Dec. 2, 2018 5:11 PM), https://www.wsj.com/amp/articles/marriotts-starwood-missed-chance-to-detect-huge-data-breach-years-earlier-1543788659.

[14] *Marriott Announces Starwood Guest Reservation Database Security Incident*, Marriott International: News Center (November 30, 2018), http://news.marriott.com/2018/11/marriott-announces-starwood-guest-reservation-database-security-incident/.

collected the PII stored on Marriott's networks. To date, Marriott has failed to provide a cogent picture of how the 2014-2018 Data Breach occurred and its full effects on consumers' PII and PCD information.

19. Investigators have found evidence that point to hackers with backing from a foreign government, such as China.[15] People familiar with the investigation "said the Marriott breach involved the same cloud-hosting space that Chinese state hackers have used in the past, and that one signature technique that involved hopping among servers also points to Chinese involvement."[16] Breaches traced back to Chinese hackers from 2014 share similar characteristics to the patterns found in Marriott's 2014-2018 Data Breach.[17] By failing to provide adequate protections for its customers' information, Marriott created a repository of personal data, including passport numbers and travel habits, that was a convenient target for hackers and foreign governments.[18] While the official investigation is ongoing and the hackers have yet to be officially identified, one thing is clear—Marriott's failure to secure its customers' data made it a desirable and easy target for hackers.

---

[15] Ellen Nakashima, *U.S. Investigators Point to China in Marriott Hack Affecting 500 Million Guests*, Washington Post (Dec. 11, 2018 9:53 PM), https://www.washingtonpost.com/technology/2018/12/12/us-investigators-point-china-marriott-hack-affecting-million-travelers/?wpmk=1&wpisrc=al_news__alert-economy--alert-national.

[16] *Id.*

[17] David Sanger, Nicole Perlroth, Glenn Thrush and Alan Rappeport, *Marriott Data Breach Is Traced to Chinese Hackers as U.S. Readies Crackdown on Beijing*, N.Y. Times (Dec. 11, 2018), https://www.nytimes.com/2018/12/11/us/politics/trump-china-trade.html.

[18] *Id.*

C. Marriott's Failure to Discover the 2014 to 2018 Data Breach

20. Marriott and Starwood failed to discover the breach to their database until nearly four years after unauthorized access was obtained. This failure to discover the breach was the result of negligent and unreasonable conduct on the part of Marriott. Marriott knew and had reason to know of weaknesses in the Starwood reservation database security protocols. Marriott also had reason to know of security threats to its reservations databases, yet failed to act reasonable to protect its customers' PCD and PII.

21. Prior attacks on Starwood and Marriott properties' cyber security gave Marriott and Starwood opportunities to discover the 2014-2018 Data Breach, but both Marriott and Starwood failed to thoroughly investigate those prior attacks. On November 20, 2015—four days after announcing the merger with Marriott—Starwood announced that it had recently discovered a "malware intrusion" that had affected a number of point of sale systems at a number of Starwood hotels in North America ("2015 Breach").[19] This breach lasted for approximately eight months before it was detected and collected data from more than 100 hotels.[20]

[19] Letter from Sergio Rivera, Americas President, Starwood Hotels & Resorts, Letter from Our President (November 20, 2015), *available at* https://www.starwoodhotels.com/Media /PDF/Corporate/Letter_1.pdf.

[20] Robert McMillan, *Marriott's Starwood Missed Chance to Detect Huge Data Breach Years Earlier, Cybersecurity Specialists Say*, Wall Street Journal (Dec. 2, 2018 5:11 PM), https://www.wsj.com/amp/articles/marriotts-starwood-missed-chance-to-detect-huge-data-breach-years-earlier-1543788659.

22. Starwood represented to its customers that after discovering the 2015 Breach, it engaged "third party forensic experts to conduct and extensive investigation."[21] Starwood also represented that it had "no indication at this time that our guest reservation or Starwood Preferred Guest membership systems were impacted."[22] Finally, Starwood stated, "We want to assure you that protecting the security of our customers' personal information is a top priority for Starwood."[23] However, Starwood did not discover the 2014-2015 Data Breach whole investigating the 2015 Breach.

23. Upon information and belief, Marriott, then Starwood, should have completed a more thorough investigation into the 2015 Breach, which would have uncovered the 2014-2018 Breach much sooner. According to Gus Hosein, executive director of Privacy International, "It's astonishing how long it took them to discover they were breached. For four years, data was being pilfered out of the company and they didn't notice. They can say all they want that they take security seriously, but they don't if you can be hacked over a four-year period without noticing."[24]

[21] Letter from Sergio Rivera, Americas President, Starwood Hotels & Resorts, Letter from Our President (November 20, 2015), *available at* https://www.starwoodhotels.com/Media /PDF/Corporate/Letter_1.pdf.
[22] *Id.*
[23] *Id.*
[24] Nicole Perlroth, Amie Tsang & Adam Stariano, *Marriott Hacking Exposes Data of Up to 500 Million Guests*, N.Y. Times (Nov. 30, 2018), https://www.nytimes.com/2018/11/30/ business/marriott-data-breach.html.

24. Marriott was aware of the 2015 Breach before any merger agreement with Starwood was reached.[25] Marriott conducted several months of due diligence into the privacy and data security of Starwood as part of its valuation of Starwood.[26] On information and belief, Marriott knew of a number of vulnerabilities within the Starwood data protection programs, but moved forward with the acquisition despite these vulnerabilities.

25. Yet another breach indicated to Marriott that its protection of guest information was inadequate, and Marriott again failed to fully investigate its systems for further malware intrusion. On August 15, 2016, another data breach involving both Marriott and Starwood hotels was announced ("2016 Breach"). A total of 12 Starwood properties and 6 Marriott properties were affected by the installation of malware by unauthorized individuals on payment processing systems.[27] This breach occurred from

[25] Robin Sidel & Craig Karmin, *Starwood Reports Payment-Information Data Breach*, Wall Street Journal (Nov. 20, 2015 5:40 PM), https://www.wsj.com/articles/starwood-reports-payment-information-data-breach-1448033469.

[26] Nicole Perlroth, Amie Tsang & Adam Stariano, *Marriott Hacking Exposes Data of Up to 500 Million Guests*, N.Y. Times (Nov. 30, 2018), https://www.nytimes.com/2018/11/30/ business/marriott-data-breach.html; Sean O'Neil, *Marriot's Starwood Data Breach Joins a Decade-Long List of Hotel Data Exposures*, Skift (Nov. 30, 2018 2:30 PM), https:// skift.com/2018/11/30/marriotts-starwood-data-breach-joins-a-decade-long-list-of-hotel-data-exposures/.

[27] Brett Molina, *Hotel Operator Hit By Data Breach*, USA Today (Aug. 1, 2016 10:50 AM), https://www.usatoday.com/story/teh/news/2016/08/15/major-hotel-operator-hit-data-breach/88753160/; *Starwood, Marriott and Hyatt Breached (Again)*, PYMNTS.com (Aug. 15, 2016), https://www.pymnts.com/news/security-and-risk/2016/hei-data-breach-starwood-marriott-hyatt/.

March of 2015 until June of 2016.[28] Upon information and belief, Marriott again failed to investigate its data protection systems and once again failed to discover the 2014-2018 Data Breach.

26. In addition to its history of data breaches, Marriott had reason to know that its data protection systems were vulnerable to attack due to the ongoing attacks on databases maintained by similarly situated companies in the hospitality industry and due to the characteristics inherent to Starwood's reservation system.

27. Other hoteliers have suffered similar attacks on their database systems. It is well known and the subject of many media reports that PII data is highly coveted and a frequent target of hackers. PII data is often easily taken because it may be less protected and regulated than payment card data. The hospitality industry, especially hotels, are perfect targets for hackers because of the wealth of financial and personal information stored in the payment and reservation systems.[29] "It is also a highly fragmented business in which large companies such as Marriott and Hilton Worldwide Holdings Inc. largely license their brands to property owners who manage the hotels."[30] Numerous other hotel chains, including Hilton, Starwood (previously), Kimpton, Mandarin Oriental, White Lodging (on two occasions), and the Trump Collection, have been hit with similar data

[28] *Starwood, Marriott and Hyatt Breached (Again)*, PYMNTS.com (Aug. 15, 2016), https://www.pymnts.com/news/security-and-risk/2016/hei-data-breach-starwood-marriott-hyatt/.
[29] Aisha Al-Muslin, Dustin Volz, & Kimberly Chin, *Marriott Says Starwood Data Breach Affects Up to 500 Million People*, Wall Street Journal (Nov. 30, 2018 8:02 PM), https://www.wsj.com/articles/marriotts-says-up-to-500-million-affected-by-starwood-breach-1543587121.
[30] *Id.*

breaches. In addition, in 2008 and 2009, hackers attacked Wyndham Worldwide's network and property management system three times.[31] The hackers were able to access data on more than 619,000 accounts and the theft of customer information resulted in what was later estimated to be $10.6 million in fraudulent charges.[32]

28. Moreover, Marriott—along with the other hotel chains that were hacked—was aware, or should have been aware, of the federal government's heightened interest in securing consumers' PII due to the very public litigation commenced by the Federal Trade Commission against Wyndham Worldwide Corporation founded upon that company's failure to provide reasonable cybersecurity protections for customer data. Despite this well-publicized litigation and the frequent public announcements of data breaches by retailers and hotel chains, Marriott opted to maintain an insufficient and inadequate system to protect the PII of Plaintiffs and members of the Class.

29. Starwood's reservation database was an inherently attractive target for hackers. In 2011, Starwood finished a decade long project to upgrade its reservation system.[33] The finished product was a massive centralized database used to book and hold reservations across nearly 1,300 properties, under different brands in close to 100

[31] Sean O'Neil, *Marriot's Starwood Data Breach Joins a Decade-Long List of Hotel Data Exposures*, Skift (Nov. 30, 2018 2:30 PM), https://skift.com/2018/11/30/marriotts-starwood-data-breach-joins-a-decade-long-list-of-hotel-data-exposures/.
[32] *Id.*
[33] Robert McMillan, *Marriott's Starwood Missed Chance to Detect Huge Data Breach Years Earlier, Cybersecurity Specialists Say*, Wall Street Journal (Dec. 2, 2018 5:11 PM), https://www.wsj.com/amp/articles/marriotts-starwood-missed-chance-to-detect-huge-data-breach-years-earlier-1543788659.

countries.[34] Such a global computer network is difficult to secure, especially because the hotels use a range of different payment and property-management systems that were assembled from Starwood's many acquisitions.[35]

30. Marriott, and by extension the Starwood database, was also a prime target for the 2014-2018 Data Breach because Marriott gathers massive amounts of private information from its guests. Marriott states the amount and types of data collected in its privacy policy:

> At touchpoints throughout your guest journey, we collect Personal Data in accordance with law, such as:
>
> - Name
> - Gender
> - Postal address
> - Telephone number
> - Email address
> - Credit and debit card number or other payment data
> - Financial information in limited circumstances
> - Language preference
> - Date and place of birth
> - Nationality, passport, visa or other government-issued identification data
> - Important dates, such as birthdays, anniversaries and special occasions
> - Membership or loyalty program data (including co-branded payment cards, travel partner program affiliations)
> - Employer details
> - Travel itinerary, tour group or activity data
> - Prior guest stays or interactions, goods and services purchased, special service and amenity requests
> - Geolocation information

[34] *Id.*
[35] *Id.*

- Social media account ID, profile photo and other data publicly available, or data made available by linking your social media and loyalty accounts

In more limited circumstances, we also may collect:

- Data about family members and companions, such as names and ages of children
- Biometric data, such as digital images
- Images and video and audio data via: (a) security cameras located in public areas, such as hallways and lobbies, in our properties; and (b) body-worn cameras carried by our loss prevention officers and other security personnel
- Guest preferences and personalized data ("Personal Preferences"), such as your interests, activities, hobbies, food and beverage choices, services and amenities of which you advise us or which we learn about during your visit[36]

31. Marriott received a benefit from storing such massive amounts of PII and PCD on its servers by utilizing this information to maximize its profits through predictive marketing and other marketing techniques.

32. Despite all the publicly available knowledge of the continued compromises of PII and PCD in the hands of unauthorized third parties, especially from entities within the hospitality industry, Marriott failed to implement adequate, reasonable, and competent security measures for detecting and preventing such attacks as the 2014-2018 Data Breach.

33. Consumers place value in data privacy and security, and they consider it when making decisions on where to stay for travel. Plaintiffs would not have stayed at the Starwood hotels nor would they have used their debit or credit cards to pay for their

[36] Privacy Center, Marriott International, https://www.marriott.com/about/privacy.mi (last visited Dec. 6, 2018.)

Starwood stays had they known that Marriott does not take all necessary precautions to secure the personal and financial data given to it by consumers.

34. Marriott failed to disclose its negligent and insufficient data security practices and consumers relied on or were misled by this omission into paying, or paying more, for accommodations at Starwood, which are branded as luxury accommodations. Marriott's failure to reasonably maintain the security of Plaintiffs' and Class Members' PII and PCD, and failure to discover the 2014-2018 breach prior to September of 2018 was careless, reckless, or at the very least, negligent.

D. Plaintiffs' Damages from Marriott's Failure to Secure Customer Data

35. The 2014-2018 Data Breach was a direct and proximate result of Marriott's failure to properly safeguard and protect Plaintiffs' and Class Members' Private Information from unauthorized access, use, and disclosure, as required by various state and federal regulations, industry practices, and the common law, including Marriott's failure to establish and implement appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of Plaintiffs' and Class Members' PII and PCD to protect against reasonably foreseeable threats to the security or integrity of such information.

36. Plaintiffs' and Class members' PII and PCD are private and sensitive in nature and was left inadequately protected by Marriott, which resulted in unauthorized exposure to third persons.

37. As a direct and proximate result of Marriott's wrongful action and inaction and the resulting 2014-2018 Data Breach, Plaintiffs and members of the Class

have been placed at an imminent, immediate, and continuing increased risk of harm from identity theft and identity fraud, requiring them to take the time and effort to mitigate the actual and potential impact of the 2014-2018 Data Breach on their lives including, *inter alia*, by placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, and closely reviewing and monitoring their credit reports and accounts for unauthorized activity.

38. In addition, there may be a time lag between when harm occurs versus when it is discovered. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[37]

Thus, Plaintiffs and Class Members may have to live in apprehension of fraud for months or years before any such fraud occurs. Further, there is often a delay between the actual fraud or identity theft being committed and the discovery of the financial damage caused by the fraudulent activity.

39. Plaintiffs and members of the Class now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. Class Members are incurring and will continue to incur such damages in addition to

[37] GAO, Report to Congressional Requesters, at p.33 (June 2007), http://www.gao.gov/new.items/d07737.pdf.

any fraudulent credit and debit card charges incurred by them and the resulting loss of use of their credit and access to funds, whether the credit card companies ultimately reimburse such charges.

40. Marriott's wrongful actions and inaction directly and proximately caused the theft and dissemination into the public domain of Plaintiffs' and Class Members' PII and PCD, causing them to suffer, and continue to suffer, economic damages and other actual harm for which they are entitled to compensation, including:

a. theft of their personal and financial information;

b. the imminent and certainly impending injury flowing from potential fraud and identify theft posed by their passport, credit/debit card, and personal information being placed in the hands of criminals;

c. the untimely and inadequate notification of the 2014-2018 Data Breach;

d. the improper disclosure of their Private Information;

e. loss of privacy;

f. ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the 2014-2018 Data Breach;

g. ascertainable losses in the form of deprivation of the value of their PII and PCD, for which there is a well-established national and international market;

h. overpayments to Marriott for products and services purchased during the 2014-2018 Data Breach in that a portion of the price paid for such products and services by Plaintiffs and members of the Class to Marriott was for the costs of reasonable and adequate safeguards and security measures that would protect customers' PII and PCD, which Marriott did not implement and, as a result, Plaintiff and members of the Class did not receive what they paid for and were overcharged by Marriott;

i. loss of use of and access to their account funds and costs associated with inability to obtain money from their accounts or being limited in the amount of money they were permitted to obtain from their accounts; and

j. deprivation of rights they possess under the various state statutes.

41. While the PII and PCD of Plaintiffs and members of the Class has been exposed due to the 2014-2018 Data Breach, the same or a copy of the PII and PCD continues to be held by Marriott. Plaintiffs and members of the Class have an undeniable interest in insuring that this information is made secure and is not subject to further theft.

V. CLASS ALLEGATIONS

42. Plaintiffs bring this action pursuant to Rules 23(a), 23(b)(2), and 23(b)(3) of the Federal Rules of Civil Procedure on behalf of themselves and all others similarly situated.

43. Plaintiffs seek to represent a class ("the Nationwide Class") defined as follows:

- All residents of the United States whose personal and/or financial information was disclosed as a result of the data breach revealed by Marriott on November 30, 2018 (the "Nationwide Class").

44. Plaintiffs also respectively seek to represent the following statewide classes ("the Statewide Classes") defined as follows:

- All residents of the State of Maryland whose personal and/or financial information was disclosed as a result of the data breach revealed by Marriott on November 30, 2018 (the "Maryland State Class").
- All residents of the State of Florida whose personal and/or financial information was disclosed as a result of the data breach revealed by Marriott on November 30, 2018 (the "Florida State Class").
- All residents of the State of North Carolina whose personal and/or financial information was disclosed as a result of the data breach revealed by Marriott on November 30, 2018 (the "North Carolina State Class").

45. Excluded from each of the Class are (a) Marriott, including any entity in which Marriott has a controlling interest, is a parent or subsidiary, or which is controlled by Marriott; (b) the officers, directors, affiliates, legal representatives, heirs, predecessors, successors, and assigns of Marriott; and (c) the judges and court personnel in this case and any members of their immediate families. Plaintiffs reserve the right to amend the Class definition if discovery and/or further investigation reveal that it should

be modified.

46. **Numerosity – Federal Rule of Civil Procedure 23(a)(1).** The members of the Class are so numerous that the joinder of all members is impractical. While the exact number of Class members is unknown to Plaintiffs at this time, Marriott has acknowledged that information of over 500 million customers may have been compromised.

47. **Commonality and Predominance – Federal Rule of Civil Procedure 23(a)(2) and 23(b)(3).** There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class members. These common questions of law and fact include, without limitation:

a. Whether Marriott owed a duty to Plaintiffs and members of the Class to safeguard and protect the security of their PII and PCD information;

b. Whether Marriott took reasonable steps and measures to safeguard and protect Plaintiffs' and members of the Class's PII and PCD information;

c. Whether Marriott had a duty to promptly notify Plaintiffs and members of the Class that their PII and PCD was, or potentially could be, compromised;

d. Whether Marriott notified Plaintiffs and members of the Class in a reasonable manner, in the most expedient time possible and without unreasonable delay that their PII and PCD had been compromised;

e. Whether Marriott violated the various state Deceptive and Unfair Trade Practices Acts by failing to implement reasonable security procedures and practices;

f. Whether Marriott violated laws by failing to promptly notify members of the Class their personal information had been compromised;

g. Whether Marriott has an implied contractual obligation to use reasonable security measures;

h. Whether Marriott has complied with any implied contractual obligation to use reasonable security measures;

i. What security measures, if any, must be implemented by Marriott to comply with its implied contractual obligations;

j. Whether members of the Class may obtain injunctive relief against Marriott under privacy laws to require that it safeguard or destroy, rather than retain, the Private Information of Plaintiffs and members of the Class;

k. Which security procedures and which data-breach notification procedure should Marriott be required to implement as part of any injunctive relief ordered by the Court;

l. Whether Marriott violated state privacy laws in connection with the actions described herein; and

m. What the nature of the relief should be, including equitable relief, to

which Plaintiffs and members of the Class are entitled.

48. All members of the proposed Class are readily ascertainable. Marriott has access to addresses and other contact information for members of the Class, which can be used for providing notice to Class members.

49. **Typicality – Federal Rule of Civil Procedure 23(a)(3)**. Plaintiffs' claims are typical of those of other Class members because Plaintiffs' information, like that of every other Class Member, was misused and/or improperly disclosed by Marriott to a third party.

50. **Adequacy of Representation – Federal Rule of Civil Procedure 23(a)(4)**. Plaintiffs will fairly and adequately represent and protect the interests of the members of the Class. Plaintiffs' Counsel are competent and experienced in litigating class actions, and Plaintiffs intend to prosecute this action vigorously.

51. **Superiority – Federal Rule of Civil Procedure 23(b)(3)**. A class action is superior to other available methods for the fair and efficient adjudication of this controversy since joinder of all the members of the Class is impracticable. Furthermore, the adjudication of this controversy through a class action will avoid the possibility of inconsistent and potentially conflicting adjudication of the asserted claims. There will be no difficulty in the management of this action as a class action, and disposition of the claims of the Class in a single action will provide substantial benefits to all parties and to the Court.

52. Damages for any individual class member are likely insufficient to justify the cost of individual litigation, so that in the absence of class treatment, Marriott's

violations of law inflicting substantial damages in the aggregate would go un-remedied without certification of the Class.

53. Class certification is also appropriate under Fed. R. Civ. P. 23(a) and (b)(2), because Marriott has acted or has refused to act on grounds generally applicable to the Class, so that final injunctive relief or corresponding declaratory relief is appropriate as to the Class as a whole.

VI. CLAIMS FOR RELIEF

COUNT 1
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiffs and the Nationwide Class)

54. Plaintiffs incorporate the substantive allegations contained throughout their Complaint as if fully set forth herein.

55. Marriott solicited and invited Plaintiffs and members of the Class to book hotel rooms at one of Marriott's hotels. Plaintiffs and members of the Class accepted Marriott's offers and booked hotel rooms at one of Marriott's Starwood hotels.

56. When Plaintiffs and members of the Class booked hotel rooms at one of Marriott's Starwood hotels, they were required to provide their PII and PCD to Marriott. In so doing, Plaintiffs and members of the Class entered into implied agreements with Marriott pursuant to which Marriott undertook a duty to safeguard and protect such information and made an implied contractual promise to do so.

57. Each booking by Plaintiffs and members of the Class was made pursuant to their mutually agreed-upon implied agreements with Marriott under which Marriott agreed to: (a) implement and maintain reasonable security procedures to protect

Plaintiffs' and the Class Members' personal information from unauthorized access, destruction, use, modification, or disclosure; and (b) ensure that any third parties who were provided with Plaintiffs' and the Class Members' PII and PCD had in place a reasonable and adequate system of security procedures and practices to protect Plaintiffs' and the Class Members' PII and PCD from being compromised and exposed to third parties.

58. Marriott, then Starwood, also affirmatively represented that its guest reservation and membership systems were secure after the announcement of the 2015 Breach. Marriott also certified that after the 2015 Breach "protecting the security of our customers' personal information is a top priority."[38]

59. Based on the implicit understanding and also on Marriott and Starwood's representations, Plaintiffs and members of the Class accepted the offers and provided Marriott their PII and PCD. Plaintiffs and members of the Class would not have provided and entrusted their PII and PCD to Marriott in the absence of the implied contractual promise to reasonably safeguard their PII and PCD information.

60. Plaintiffs and members of the Class fully performed their obligations under their agreements with Marriott.

61. Marriott breached the implied contractual promise that it made to Plaintiffs and members of the Class by:

a. failing to implement and maintain reasonable security procedures to

[38] Letter from Sergio Rivera, Americas President, Starwood Hotels & Resorts, Letter from Our President (November 20, 2015), *available at* https://www.starwoodhotels.com/Media /PDF/Corporate/Letter_1.pdf.

protect Plaintiffs' and the Class Members' PII and PCD from unauthorized access, destruction, use, modification, or disclosure; and

b. failing to ensure that any third parties who were provided with Plaintiffs' and the Class Members' PII and PCD had in place a reasonable and adequate system of security, PCD procedures and practices to protect Plaintiffs' and the Class Members' PII from being compromised and exposed to third parties.

62. Plaintiffs and members of the Class have lost the benefit of their bargain with Marriott by having their PII and PCD compromised and exposed and have been placed at an imminent, immediate, and continuing risk of identity theft-related harm.

63. As a direct and proximate result of Marriott's breaches of the implied contractual promises alleged herein, Plaintiffs and members of the Class sustained actual losses and damages in an amount according to proof at trial but in excess of the minimum jurisdictional requirement of this Court.

COUNT 2
NEGLIGENCE
(On Behalf of Plaintiffs and the Nationwide Class)

64. Plaintiffs incorporate the substantive allegations contained throughout their Complaint as if fully set forth herein.

65. Marriott owes numerous duties to Plaintiffs and the other members of the Class. These duties include duties:

a. to exercise reasonable care in obtaining, retaining, securing,

safeguarding, deleting, and protecting its customers' PII and PCD in its possession;

b. to protect customers' PII and PCD in its possession using reasonable and adequate security procedures that are compliant with industry-standard practices; and

c. to implement processes to quickly detect a data breach and to timely act on warnings about data breaches, including promptly notifying Plaintiffs and members of the Class of any breach.

66. Marriott knew or should have known the risks of collecting and storing its customers' PII and PCD and the importance of maintaining secure payment systems. Marriott knew or should have known of the many breaches that targeted other businesses in the years before the 2014-2018 Data Breach announced on November 30, 2018.

67. Marriott knew or should have known that its reservation systems did not adequately safeguard Plaintiffs' and the other Class Members' PII and PCD.

68. Marriott breached the duties it owes to Plaintiffs and members of the Class in several ways, including:

a. failing to implement adequate security systems, protocols and practices sufficient to protect customer Private Information and thereby creating a foreseeable risk of harm;

b. failing to comply with the minimum industry data security standards during the period of the data breach; and

c. failing to timely and accurately disclose to customers that their

Private Information had been improperly acquired or accessed.

69. But for Marriott's wrongful and negligent breach of the duties it owed to Plaintiffs and members of the Class, their PII and PCD would not have been compromised.

70. The injury and harm that Plaintiffs and members of the Class suffered was the direct and proximate result of Marriott's negligent conduct.

71. The law also imposes an affirmative duty on Marriott to timely disclose the theft of the PII and PCD so that Plaintiffs and members of the Class can be vigilant in attempting to determine if any of their accounts or assets have been stolen through identity theft. Through its failure to provide timely and clear notification of the data breach to consumers, Marriott negligently prevented Plaintiffs and members of the Class from taking meaningful, proactive steps to investigate possible identity theft. As a direct and proximate cause of failing to use appropriate security practices, Marriott's system was hacked causing Plaintiffs' and all Class Members' PII and PCD to be compromised by unauthorized individuals.

72. The breach of the security system caused direct and substantial damages to Plaintiffs and members of the Class, as well as the possibility of future harm through the dissemination of private information and possibility of credit fraud or identity theft.

73. For all the reasons stated above, Marriott's conduct was negligent and departed from reasonable standards of care including, but not limited to:

a. failing to adequately protect the PII and PCD;

b. failing to conduct regular and reasonably thorough security audits;

c. failing to adequately investigate earlier breaches to its system;

d. failing to provide adequate and appropriate supervision of persons having access to Plaintiffs and Class Members' PII and PCD; and

e. failing to provide Plaintiffs and members of the Class with timely and sufficient notice that their sensitive PII and PCD had been compromised.

74. Neither Plaintiffs nor the other members of the Class contributed to the 2014-2018 Data Breach or subsequent misuse of their PII and PCD as described in this Complaint. As a direct and proximate result of Marriott's actions and inactions, Plaintiffs and every member of the Class has been put at risk of credit fraud and/or identity theft. Marriott is also liable to those Class Members who have directly sustained damages as a result of identity theft or other unauthorized use of their PII and PCD.

COUNT 3
NEGLIGENCE PER SE
(On Behalf of Plaintiffs and the Nationwide Class)

75. Plaintiffs incorporate the substantive allegations contained throughout their Complaint as if fully set forth herein.

76. Marriott also had a duty arising under Section 5 of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45, to provide fair and adequate computer systems and data security to safeguard the personal information, including PII and PCD, of Plaintiffs and members of the Class. The FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect personal and confidential

information. Various FTC publications and data security breach orders further form the basis of Marriott's duty. In addition, individual states have enacted statutes based upon the FTC Act that also created a duty.

77. Marriott solicited, gathered, and stored personal information, including PII and PCD, of Plaintiffs and members of the Class to facilitate sales transactions which affect commerce.

78. Upon information and belief, Marriott improperly and inadequately safeguarded the PII and PCD of Plaintiffs and members of the Class in deviation from standard industry rules, regulations, and practices at the time of the 2014-2018 Data Breach. Marriott violated the FTC Act by failing to use reasonable measures to protect personal information of Plaintiffs and members of the Class and by not complying with applicable industry standards, as described herein.

79. Plaintiffs and members of the Class are within the class of persons that the FTC Act was intended to protect.

80. The harm that occurred as a result of the 2014-2018 Data Breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiffs and members of the Class.

81. Marriott's failure to take proper security measures to protect Plaintiffs' and Class Members' sensitive PII and PCD has caused Plaintiffs and members of the Class to suffer injury and damages. As described herein, Plaintiffs received notice that

their information was compromised, and now must take and have taken affirmative steps to ensure that their identity is not stolen and their financial information is not compromised. In addition, Class Members' accounts have been cancelled, suspended, or otherwise rendered unusable as a result of the 2014-2018 Data Breach and resulting fraudulent charges. Class Members have also had to pay late fees and spend valuable time and effort scrutinizing their accounts, and communicating with their financial institutions to dispute fraudulent charges.

COUNT 4
MARYLAND PERSONAL INFORMATION PROTECTION ACT
Md. Comm. Code §§ 14-3501, *et seq.*
(On Behalf of Plaintiffs and the Maryland State Class)

82. Plaintiffs incorporate the substantive allegations contained throughout their Complaint as if fully set forth herein.

83. Under Md. Comm. Code § 14-3503(a), "[t]o protect Personal Information from unauthorized access, use, modification, or disclosure, a business that owns or licenses Personal Information of an individual residing in the State shall implement and maintain reasonable security procedures and practices that are appropriate to the nature of Personal Information owned or licensed and the nature and size of the business and its operations."

84. Marriott is a business that owns or licenses computerized data that includes Personal Information as defined by Md. Comm. Code §§ 14-3501(b)(1) and (2).

85. Plaintiffs and members of the Class are "individuals" and "customers" as defined and covered by Md. Comm. Code §§ 14-3502(a) and 14-3503.

86. Plaintiffs' and Class Members' Private Information, as described herein and throughout and PII and PCD, includes Personal Information as covered under Md. Comm. Code § 14-3501(d).

87. Marriott did not maintain reasonable security procedures and practices appropriate to the nature of the Personal Information owned or licensed and the nature and size of its business and operations in violation of Md. Comm. Code § 14-3503.

88. The 2014-2018 Data Breach was a "breach of the security of a system" as defined by Md. Comm. Code § 14-3504(1).

89. Under Md. Comm. Code § 14-3504(b)(1), "[a] business that owns or licenses computerized data that includes Personal Information of an individual residing in the State, when it discovers or is notified of a breach of the security system, shall conduct in good faith a reasonable and prompt investigation to determine the likelihood that Personal Information of the individual has been or will be misused as a result of the breach."

90. Under Md. Comm. Code §§ 14-3504(b)(2) and 14-3504(c)(2), "[i]f, after the investigation is concluded, the business determines that misuse of the individual's Personal Information has occurred or is reasonably likely to occur as a result of a breach of the security system, the business shall notify the individual of the breach" and that notification "shall be given as soon as reasonably practical after the business discovers or is notified of the breach of a security system."

91. Because Marriott discovered a security breach and had notice of a security breach, Marriott had an obligation to disclose the 2014-2018 Data Breach in a timely and

accurate fashion as mandated by Md. Comm. Code §§ 14-3504(b)(2) and 14-3504(c)(2).

92. By failing to disclose the 2014-2018 Data Breach in a timely and accurate manner, Marriott violated Md. Comm. Code §§ 14-3504(b)(2) and 14-3504(c)(2).

93. As a direct and proximate result of Marriott's violations of Md. Comm. Code §§ 14-3504(b)(2) and 14-3504(c)(2), Plaintiffs and members of the Class suffered damages, as described above.

94. Pursuant to Md. Comm. Code § 14-3508, Marriott's violations of Md. Comm. Code §§ 14-3504(b)(2) and 14-3504(c)(2) are unfair or deceptive trade practices within the meaning of the Maryland Consumer Protection Act, 13 Md. Comm. Code §§ 13-101, et seq. and subject to the enforcement and penalty provisions contained within the Maryland Consumer Protection Act.

95. Plaintiffs and Class Members seek relief under Md. Comm. Code §13-408, including actual damages and attorney's fees.

COUNT 5
MARYLAND CONSUMER PROTECTION ACT,
Md. Comm. Code §§ 13-301, *et seq.*
(On Behalf of Plaintiffs and the Maryland State Class)

96. Plaintiffs incorporate the substantive allegations contained throughout their Complaint as if fully set forth herein.

97. Maryland's Consumer Protection Act ("MCPA") § 13-303(1) prohibits "unfair or deceptive trade practices" in a variety of circumstances, including the "sale . . . of consumer good . . . or consumer services." The statute lists various ways of committing unfair or deceptive trade practices. For example, a violation may involve an affirmative "false ... or misleading oral or written statement ... or other representation of

any kind which has the capacity, tendency, or effect of deceiving or misleading consumers." Section 13.301(2)(iv) states that prohibited representations include representations that "Consumer goods, . . . or consumer services have a sponsorship, approval, accessory, characteristic, ingredient, use, benefit, or quantity which they do not have," CL §13-301(2)(i), and "Consumer goods, consumer realty, or consumer services are of a particular standard, quality, grade, style, or model which they are not."

98. A violation may also consist of an omission — i.e., a "failure to state a material fact if the failure deceives or tends to deceive." CL §13-301(3). It is not necessary that a consumer actually have been misled or damaged as a result of the practice. CL §13-302. The Act also prohibits "Deception, fraud, false pretense, false premise, misrepresentation, or knowing concealment, suppression, or omission of any material fact with the intent that the consumer rely on the same in connection with … (i) the promotion or sale of any consumer goods…." *Id.* at 13. The Act is to be construed liberally to promote the protection of consumers. CL §§13-105, 13-102(3).

99. Marriott is a "person" as defined by Md. Comm. Code § 13-101(h).

100. Marriott's conduct as alleged herein related to "sales," "offers for sale," or "bailment" as defined by Md. Comm. Code § 13-101(i) and § 13-303.

101. Plaintiffs and members of the Class are "consumers" as defined by Md. Comm. Code § 13-101(c).

102. Marriott advertises, offers, or sells "consumer goods" or "consumer services" as defined by Md. Comm. Code § 13-101(d).

103. Marriott advertised, offered, or sold goods or services in Maryland and

engaged in trade or commerce directly or indirectly affecting the people of Maryland.

104. Marriott engaged in unfair and deceptive trade practices, in violation of Md. Comm. Code § 13-301, including:

a. False or misleading oral or written representations that have the capacity, tendency, or effect of deceiving or misleading consumers;

b. Failing to state a material fact where the failure deceives or tends to deceive;

c. Advertising or offering consumer goods or services without intent to sell, lease, or rent them as advertised or offered;

d. Deception, fraud, false pretense, false premise, misrepresentation, or knowing concealment, suppression, or omission of any material fact with the intent that a consumer rely on the same in connection with the promotion or sale of consumer goods or services or the subsequent performance with respect to an agreement, sale lease or rental.

105. Marriott engaged in these unfair and deceptive trade practices in connection with offering for sale or selling consumer goods or services or with respect to the extension of consumer credit, in violation of Md. Comm. Code § 13-303, including:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs and Class Members' personal and confidential information, which was a direct and proximate cause of the 2014-2018 Data Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the 2014-2018 Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Class Members' personal and confidential information, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, the GLBA, 15 U.S.C. § 6801, et seq., and the Maryland Personal Information Protection Act, Md. Comm. Code § 14-3503, which was a direct and proximate cause of the 2014-2018 Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiffs' and Class Members' personal and confidential information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Class Members' information, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, the GLBA, 15 U.S.C. § 6801, et seq., and the Maryland Personal Information Protection Act, Md. Comm. Code § 14- 3503;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs' and Class Members' information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Class Members' information, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, the GLBA, 15 U.S.C. § 6801, et seq., and the Maryland Personal Information Protection Act, Md. Comm. Code § 14-3503.

106. Marriott's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Marriott's data security and ability to protect the confidentiality of consumers' personal and confidential information. Marriott's misrepresentations and omissions would have been important to a significant number of consumers in making financial decisions.

107. Marriott intended to mislead Plaintiffs and members of the Class and induce them to rely on their misrepresentations and omissions.

108. Had Marriott disclosed to Plaintiffs and members of the Class that its data systems were not secure and, thus, vulnerable to attack, Marriott would have been forced to adopt reasonable data security measures and comply with the law.

109. Marriott acted intentionally, knowingly, and maliciously to violate Maryland's Consumer Protection Act, and recklessly disregarded Plaintiffs' and Class

Members' rights. Marriott was on notice of the possibility of the 2014-2018 Data Breach due to its prior data breach and infiltrations of its systems.

110. As a direct and proximate result of Marriott's unfair and deceptive acts and practices, Plaintiffs and members of the Class have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Personal Information.

111. Plaintiffs and Class Members seek all monetary and non-monetary relief allowed by law, including damages, disgorgement, injunctive relief, and attorneys' fees and costs.

COUNT 6
FLORIDA DECEPTIVE AND UNFAIR TRADE PRACTICES ACT
Fla. Stat. §§ 501.201, et seq.
(On Behalf of Plaintiff Kathleen Frakes Hevener and the Florida State Class)

112. Plaintiff Hevener incorporates the substantive allegations contained throughout her Complaint as if fully set forth herein.

113. Plaintiff Hevener and Florida State Class members are "consumers" as defined by Fla. Stat. § 501.203.

114. Marriott advertised, offered, or sold goods or services in Florida and engaged in trade or commerce directly or indirectly affecting the people of Florida.

115. Marriott engaged in unconscionable, unfair, and deceptive acts and practices in the conduct of trade and commerce, in violation of Fla. Stat. § 501.204(1),

including:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Class Members' personal and confidential information, which was a direct and proximate cause of the 2014-2018 Data Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the 2014-2018 Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Class Members' personal and confidential information, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, the GLBA, 15 U.S.C. § 6801, et seq., and the Florida's data security statute, F.S.A. § 501.171(2), which was a direct and proximate cause of the 2014-2018 Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff's and Class Members' personal and confidential information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and

statutory duties pertaining to the security and privacy of Plaintiff's and Class Members' information, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, the GLBA, 15 U.S.C. § 6801, et seq., and the Florida's data security statute, F.S.A. § 501.171(2);

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff's and Class Members' information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Class Members' information, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, the GLBA, 15 U.S.C. § 6801, et seq., and the Florida's data security statute, F.S.A. § 501.171(2).

116. Marriott's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Marriott's data security and ability to protect the confidentiality of consumers' personal and confidential information. Marriott's misrepresentations and omissions would have been important to a significant number of consumers in making financial decisions.

117. Marriott intended to mislead Plaintiff and members of the Class and induce them to rely on their misrepresentations and omissions.

118. Had Marriott disclosed to Plaintiff and members of the Class that its data

systems were not secure and, thus, vulnerable to attack, Marriott would have been forced to adopt reasonable data security measures and comply with the law.

119. Marriott acted intentionally, knowingly, and maliciously to violate Florida's Deceptive and Unfair Trade Practices Act, and recklessly disregarded Plaintiff and Class Members' rights. Marriott was on notice of the possibility of the 2014-2018 Data Breach due to its prior data breach and infiltrations of its systems.

120. As a direct and proximate result of Marriott's unfair and deceptive acts and practices, Plaintiff and members of the Class have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Personal Information.

121. Plaintiff and members of the Class seek all monetary and non-monetary relief allowed by law, including damages, disgorgement, injunctive relief, and attorneys' fees and costs.

COUNT 7
NORTH CAROLINA IDENTITY THEFT PROTECTION ACT
N.C. Gen. Stat. §§ 75-60, et seq.
(On Behalf of Plaintiff Tamara Wallace and the North Carolina State Class)

122. Plaintiffs incorporate the substantive allegations contained throughout their Complaint as if fully set forth herein.

123. Marriott is a business that owns or licenses computerized data that includes Personal Information as defined by N.C. Gen. Stat. § 75-61(1).

124. Plaintiff Tamara Wallace and North Carolina State Class members are "consumers" as defined by N.C. Gen. Stat. § 75-61(2).

125. Marriott is required to accurately notify Plaintiff Wallace and North Carolina State Class members if it discovers a security breach, or receives notice of a security breach (where unencrypted and unredacted Personal Information was accessed or acquired by unauthorized persons), without unreasonable delay under N.C. Gen. Stat. § 75-65.

126. Plaintiff and North Carolina State Class members' PII and PCD includes Personal Information as covered under N.C. Gen. Stat. § 75-61(10).

127. Because Marriott discovered a security breach and had notice of a security breach (where unencrypted and unredacted Personal Information was accessed or acquired by unauthorized persons), Marriott had an obligation to disclose the 2014-2018 Data Breach in a timely and accurate fashion as mandated by N.C. Gen. Stat. § 75-65.

128. By failing to disclose the 2014-2018 Data Breach in a timely and accurate manner, Marriott violated N.C. Gen. Stat. § 75-65.

129. A violation of N.C. Gen. Stat. § 75-65 is an unlawful trade practice under N.C. Gen. Stat. Art. 2A § 75-1.1.

130. As a direct and proximate result of Marriott's violations of N.C. Gen. Stat. § 75-65, Plaintiff and North Carolina State Class members suffered damages, as described above.

131. Plaintiff and North Carolina State Class members seek relief under N.C. Gen. Stat. §§ 75-16 and 16.1, including treble damages and attorney's fees.

COUNT 8
NORTH CAROLINA UNFAIR TRADE PRACTICES ACT
N.C. Gen. Stat. Ann. §§ 75-1.1, et seq.
(On Behalf of Plaintiff Tamara Wallace and the North Carolina State Class)

132. Plaintiffs incorporate the substantive allegations contained throughout their Complaint as if fully set forth herein.

133. Marriott advertised, offered, or sold goods or services in North Carolina and engaged in trade or commerce directly or indirectly affecting the people of North Carolina, as defined by N.C. Gen. Stat. Ann. § 75-1.1(b).

134. Marriott engaged in unfair and deceptive acts and practices in or affecting commerce, in violation of N.C. Gen. Stat. Ann. § 75-1.1, including:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and North Carolina State Class members' Personal Information, which was a direct and proximate cause of the 2014-2018 Data Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the 2014-2018 Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and North Carolina State Class members' Personal Information, including duties imposed by

the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, and the GLBA, 15 U.S.C. § 6801, et seq., which was a direct and proximate cause of the 2014-2018 Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and North Carolina State Class members' personal and confidential, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and North Carolina State Class members' personal and confidential, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, and the GLBA, 15 U.S.C. § 6801, et seq.;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and North Carolina State Class members' personal and confidential; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and North Carolina State Class members' personal and confidential, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, and the GLBA, 15 U.S.C. § 6801, et seq.

135. Marriott's representations and omissions were material because they were

likely to deceive reasonable consumers about the adequacy of Marriott's data security and ability to protect the confidentiality of consumers' personal and confidential.

136. Marriott intended to mislead Plaintiff and North Carolina State Class members and induce them to rely on its misrepresentations and omissions.

137. Had Marriott disclosed to Plaintiff and North Carolina State Class members that its data systems were not secure and, thus, vulnerable to attack, Marriott would have been forced to adopt reasonable data security measures and comply with the law.

138. Marriott acted intentionally, knowingly, and maliciously to violate North Carolina's Unfair Trade Practices Act, and recklessly disregarded Plaintiff and North Carolina State Class members' rights. Marriott's numerous past data breaches put it on notice that its security and privacy protections were inadequate.

139. As a direct and proximate result of Marriott's unfair and deceptive acts and practices, Plaintiff and North Carolina State Class members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their personal and confidential.

140. Marriott's conduct as alleged herein was continuous, such that after the first violations of the provisions pled herein, each week that the violations continued constitute separate offenses pursuant to N.C. Gen. Stat. Ann. § 75-8.

141. Plaintiff and North Carolina State Class members seek all monetary and non-monetary relief allowed by law, including actual damages, treble damages, and attorneys' fees and costs.

VII. REQUEST FOR RELIEF

WHEREFORE, Plaintiffs, individually and on behalf of the all Class Members, respectfully requests that the Court enter judgment in their favor and against Defendant, Marriott International, Inc., parent company to Starwood Hotels & Resorts Worldwide, LLC, as follows:

a. Declaring that this action is a proper class action, certifying the Class as defined herein, designating Plaintiffs as Nationwide Class Representatives, Plaintiffs Peter Maldini & Kathleen Frakes Hevener as Maryland Class Representatives, Plaintiff Kathleen Frakes Hevener as a Florida Class Representative, Plaintiff Tamara Wallace as a North Carolina Class Representative, and appointing Plaintiffs' counsel as Class Counsel;

b. For equitable relief enjoining Marriott from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiffs' and Class Members' personal and confidential information, and from refusing to issue prompt, complete, and accurate disclosures to the Plaintiffs and members of the Class;

c. For equitable relief compelling Marriott to utilize appropriate methods and policies with respect to consumer data collection, storage, and safety and to disclose with specificity to Class members the type of PII and PCD compromised.

d. For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Marriott's wrongful conduct;

e. For an award of actual damages and compensatory damages, in an amount to be determined;

f. For an award of costs of suit and attorneys' fees, as allowable by law; and

g. Such other and further relief as this court may deem just and proper.

VIII. JURY DEMAND

Plaintiffs hereby demand a trial by jury on all issues so triable.

DATED: December 13, 2018

/s/ *D. Bruce Poole*
D. Bruce Poole, #25784
bruce.poole@poolelg.com
THE POOLE LAW GROUP
29 W. Franklin Street
Hagerstown, Maryland 21740
Telephone: 301-790-3600
Fax: 301-714-0082

/s/ *Roland Tellis*
Roland Tellis (*pro hac vice* anticipated)
rtellis@baronbudd.com
David Fernandes (*pro hac vice* anticipated)
dfernandes@baronbudd.com
Elizabeth Smiley (*pro hac vice* anticipated)
esmiley@baronbudd.com
BARON & BUDD, P.C.
15910 Ventura Boulevard, Suite 1600
Encino, California 91436
Telephone: 818-839-9698

Plaintiffs' Counsel